REMARKS

In the Office Action, claims 1-35 were rejected. By the present Response, claim 28 is amended. Upon entry of the amendments, claims 1-35 will remain pending in the present patent application. Reconsideration and allowance of all pending claims are requested.

Claim 28 has been amended to correct inadvertent typographical and grammatical errors in the claim. No new matter has been added.

Rejections Under 35 U.S.C. § 102

In the Office Action, claims 1, 2, 5, 8, 10-13, 14-17, 19, 27 and 28-35 were rejected under 35 U.S.C. §102(b) as anticipated by Ross, Jr. et al. (U.S. Patent No. 5,823,948; hereinafter "Ross"). Applicant notes that of these claims, claims 1, 14, 27, 28 and 33 are independent. In analyzing the claims, the Examiner submitted that particular passages of Ross read on virtually all of the recitations of the independent claims. Specifically, the Examiner relied upon a passage at column 5, lines 5-10 and 34-52 of Ross. Applicant has examined all of these passages, as well as the remainder of Ross, and submits that the subject matter of at least claims 1, 14, 27, 28 and 33 is not taught by Ross.

As amended in the Request for Continued Examination, the cited claims recite in generally similar language that data is generated by a *user* and stored on a secure data depository *operative in a first processing space inaccessible to a user*. Moreover, the claims recite, in generally similar language, that a secure data file is created from this data and *provided or exported to a second processing space separated from the first processing space*.

With regards to both of these recitations, the Examiner relied heavily upon the passages from Ross. However, these passages, and the Examiner's own assertions do not

appear to address the fact that the claims recite that the *first processing space is inaccessible* to either the user or to an intended recipient of a report. Specifically, the passages relied upon by the Examiner state:

> The transcribed dictations are placed in an electronic storage bin in the communications server(s) for transferring the dictation transcriptions to the file servers, and storing the dictation transcriptions in the file servers 2 and 3 as text associated with patient data for particular patients.
>
> ...
>
> The patient record documentation method provides tracking and order entry. File servers provide data and software from the file servers through a network hub and network to multiple CPU'S. The patient data is transferred from the CPU's to the file servers. Portions of the record that are unique to particular patients are dictated. The dictation is transmitted over voice lines to a transcription center where the dictation is transcribed. The transcribed dictation is transmitted to the communication server(s), which feeds the dictation transcription to the file servers as text components. The text on particular patients is stored in the file server with the tabled data. Word and sentence generation and coordination software is stored in the peripheral CPU'S. Monitors display text sentences generated by the generation software as summaries, together with the text from the dictation transcriptions. The text summaries are sent from the peripheral CPU's to a printer via the local network for generation of printed patient textual reports with sentences generated in medical English text.

Ross, Jr. et al., col. 5, lines 5-10 and 34-52.

These passages disclose that transcribed dictations are stored with other files in the file servers 2 and 3. *See id.* Any personnel on the network may track and order these files from the file servers. *See id.* The access to the network, as described in other

passages, is only limited to personnel that demonstrate their identity to establish access to the network with specific rights in the network. *See* Ross, col. 12, lines 55-67. That is, the only limitation in access to the patient data is the modification of the patient data, which is limited to personnel who are in a certain class of users, such as the personnel that entered the data. *See id.* at col. 13, lines 5-31. As such, any user or report recipient able to connect to the network is able to access these files.

These teachings are contrary to the claim recitations because the claims require that the data is stored for the user in a *first processing space that is inaccessible to* the user or to an intended report recipient. The Examiner appears to assert that denial of access to a user to the network satisfies this recited feature. However, the mere limitation of access to the network does not provide the *first processing space that is inaccessible*. As a result, the Ross reference does not disclose or teach storing data in a processing space that is *inaccessible to the user* or an intended report recipient because any personnel can access the patient data and the personnel that entered the data can view and modify the data. As such, the Examiner's assertions are clearly not supported by the Ross reference.

With regard to the second point, the Examiner asserted that the above cited passages of Ross also disclose *accessing data to create a secure data file*. However, the Examiner failed to allege or particularly point to any specific structures or elements that correspond to the *secure data file*. Accordingly, when properly construing the claims in view of the previous discussion, Applicant submits that no structures in Ross correspond to the *secure data file* because Ross does not disclose or suggest any secure files created in or from data in a processing space inaccessible to a user or an intended report recipient. That is, the Ross reference merely describes that patient data is transferred from the CPU's, which are the peripheral devices 9, to the file servers 2 and 3. *See id.* at col. 5, lines 34-46. The patient data, which may include transcriptions of dictations in the form of text files along with other patient data, *is accessible by the user*.

The Examiner also relied upon a passage of Ross at col. 12, line 54 through col. 13, line 4. This passage reads:

> Personnel using the system must clearly demonstrate their identity using a variety of methods depending on the system configuration. Single and multiple passwords, smart card, magnetic card or other personal ID technologies. The user's identity establishes the individual "rights" to use various functions. For example, physicians may be the only users given rights to generate prescriptions, nurses could have rights to implement various medical procedures, ward clerks might need rights to order labs, but records clerks may be limited to changing demographic information. If smart cards are used, the system is available only while a proper, authorized card is inserted. Upon withdrawal, the system completes any processes and reverts to a non responding mode[.]
>
> Remote access to the system is controlled by "firewall" software routines which require varying security levels up to a forced return link initiated by the system to authorized remote computers or systems.

Ross, Jr. et al., col. 12, line 54 through col. 13 line 4.

Applicant notes in passing that as regards even the first point above relating to the inaccessibility of data in the first processing space to users that generate the data, this passage of Ross provides no useful teaching. That is, the passage simply indicates that various *controlled access* can be provided to parts of the system. However, the passage does not indicate that a first processing space is *inaccessible* to the user that generated data or to an intended recipient of a report.

As regards the extraction or export of secure data files for eventual report generation, the passage is also wanting. Nothing in the passage whatsoever would indicate that data is extracted or provided from a first processing space in the form of a

secure data file. Moreover, nothing the passage indicates that such a secure data file is provided or exported to any other processing space.

The invention recited in independent claims 1, 14, 27, 28 and 33 greatly facilitates the generation of reports from secure data. Processing spaces, well understood to those skilled in the art, are provided that are separated in terms of accessibility. The first processing space is inaccessible to users or intended report recipients. The second processing space receives a secure data file or data needed to complete a report, and the report is generated from this data. The separation of the two processing spaces facilitates reporting of the information without providing access to the secure processing space by either the user that generated the data or the intended report recipient. Nothing in Ross even remotely refers to two separate processing spaces, where a first processing space is inaccessible to either a user that generated data stored in the space or to an intended report recipient. Throughout Ross, only *controlled access* is described, and the reference clearly does not anticipate providing separate processing spaces or extracting data for report generation in the manner claimed.

Accordingly, Ross cannot anticipate claims 1, 14, 27, 28 or 33, or the claims depending therefrom. Consequently, Applicant again requests that the rejection under 35 U.S.C. §102(b) based on Ross be withdrawn and that the recited claims be allowed.

Rejections Under 35 U.S.C. § 103

Claims 3, 4, 6, 7, 9, 18 and 20-26 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ross in view of Rasansky et al. (U.S. Patent No. 5,960,406; hereinafter "Rasansky"). Of these claims, only claim 20 is independent. Applicant submits that claim 20 is clearly allowable over both Ross and Rasansky, considered separately or in combination, as are the dependent claims rejected on this basis. The claims not depending from claim 20 are clearly allowable because Rasansky does not

obviate the deficiencies of Ross outlined above. Claim 20 is clearly patentable, along with its dependent claims for the reasons summarized below.

Like the claims discussed above, claim 20 specifically recites a secure data repository operative in a first processing space for storing user-generated data, where the first processing space is inaccessible to the user. The claim also recites a data access program module that extracts report data from the secure data repository, the report data being stored in a second data repository securely separated from the first processing space. With regards to these recitations, the Examiner again relied upon the same passages outlined above from Ross. Clearly, neither these passages, nor the rest of Ross teaches these aspects of the invention. Accordingly, the rejection simply cannot stand on this basis alone.

Rasansky also does not teach these features. Indeed, the Examiner relied upon Rasansky only for disclosure of a report template stored in a "second" processing space. The Examiner then concluded that such report templates could be used to generate reports based upon data extracted from a secure processing space.

Clearly, because Ross does not teach a secure processing space or the extraction of data from such a space for report generation, the mere provision of a template by Rasansky cannot result in the invention recited in claim 20. That is, the report template of Rasansky would apparently be populated by unsecure data that could be accessed by anyone given controlled access as taught by Ross. Because Ross does not teach separation of controlled access processing spaces from other processing spaces, there would be no need to populate a report template of the type taught by Rasansky in anything other than the single processing space discussed by Ross. Accordingly, no combination of Ross and Rasansky could possibly render obvious the invention recited in claim 20.

Conclusion

In view of the remarks and amendments set forth above, Applicant respectfully requests allowance of the pending claims. If the Examiner believes that a telephonic interview will help speed this application toward issuance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Date: 11/4/2005

Patrick S. Yoder
Reg. No. 37,479
FLETCHER YODER
P.O. Box 692289
Houston, TX 77269-2289
(281) 970-4545